AU/AIR FORCE FELLOWS/NNN/2002-04

AIR FORCE FELLOWS PROGRAM

AIR UNIVERSITY

CONFRONTING AN OLD ENEMY: TERRORISM AND THE CHANGING FACE OF MILITARY INTELLIGENCE

by

JACK L. JONES, Lt Col, USAF
1433 Capri Lane #5308
Weston FL, 33326
198-52-5982

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Charles G. MacDonald

Florida International University

April 2002

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
APR 2002	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Confronting an Old Enemy: Terrorism and The Changing Face of Military Intelligence	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air University Press Maxwell AFB, AL 36112-6615**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**56**	

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US Government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States Government.

Contents

Page

Tables

Page

Acknowledgements

I want to thank my research advisor at Florida International University, Professor Charles MacDonald, for his time, patience, and invaluable contributions to my research paper. I also owe a great debt of gratitude to the senior intelligence leaders at the Defense Intelligence Agency, Joint Chiefs of Staff, United States Air Force and Federal Bureau of Investigations for allowing me to interview them for this study. To Mr. Andre, Admiral Murrett, Mr. Boyd, Mr. Duecy, Mr. Van Duyn, and Colonel Wohlman, thank you for your time and extraordinary insight into the world of terrorism and intelligence analysis. I owe a special thank you to my friend Colonel Jon Wohlman for 'opening the research doors' and facilitating the above interviews. Without him this paper could not have been written.

AU/AIR FORCE FELLOWS/NNN/2002-04

Abstract

This paper addresses the Department of Defense (DOD) all-source, analytic intelligence apparatus and assesses its efforts to combat transnational terrorism. Specifically, the author argues the DOD intelligence community requires a cultural shift to prosecute more effectively the war on terrorism and strengthen America's national security. Existing cultural biases, stove-piped operational processes, and limited analyst recruitment programs have weakened the DOD intelligence community's ability to face the twenty-first century terrorist enemy.

This study first addresses the recent history (1993-present) of the intelligence community's efforts to battle terrorism. Evidence both criticizing and supporting the intelligence community's efforts is presented, and the impact of key "intelligence gaps" and lessons learned are analyzed. From this broad survey and analysis, the author then focuses on two areas—the operational culture of DOD's analytic intelligence community and the process of intelligence analysis. Drawing from interviews with senior DOD intelligence officials, and the work of Bruce D. Berkowitz, Allan E. Goodman, Paul R. Pillar and others, the author argues operational culture and intelligence analysis are the two most critical pieces requiring change within the DOD intelligence community. Migrating the culture of the intelligence "tribe" away from a predominantly stove-piped and compartmentalized mentality is a must for future success. Equally important is enhancing the analytic process and improving access to information the military intelligence community uses to confront the technologically empowered transnational enemy.

Against this backdrop of improving American warfighting capability against terrorism, the author concludes with a number of prescriptions for the future. Key among these are improved information sharing between the various intelligence organizations within DOD; more aggressive and broad-based recruitment and training programs for the intelligence career field; increased utilization of non-traditional intelligence sources such as the Internet, American and foreign scholars, and other open-source materials; and increased and more in-depth exchanges with foreign government security and intelligence agencies.

Chapter 1

Introduction

> *Surprise attacks often succeed despite the availability of warning indicators. This pattern leads many observers to blame derelict intelligence officials or irresponsible policymakers. The sad truth is that the fault lies more in natural organizational forces, and in the pure intractability of the problem, than in the skills of spies or statesmen.*
>
> —Richard Betts from "Fixing Intelligence," 2002

The tragic events of September 11, 2001—widely labeled as a massive intelligence failure--stand as a point of departure from post-World War II United States national security policy. President Bush, in an effort to counter the spread of global terrorism, is proposing the most sweeping changes in national defense since the National Security Act of 1947.[1] Perhaps the most important theme, and certainly the most hotly-debated subject in this national security review, is the ongoing examination of the intelligence community's performance in addressing the heightened terrorist threat.

This paper explores the Department of Defense (DOD) all source, analytic intelligence apparatus and assesses its efforts to combat transnational terrorism. Existing cultural practices and compartmentalized operational processes within the DOD Intelligence Community, long successful in dealing with nation-state threats such as the former Soviet Union, were exposed on September 11 as insufficient in confronting the technologically-empowered terrorist enemy. In order to more effectively prosecute the war on terrorism and strengthen America's national

security, the DOD Intelligence Community requires a cultural shift to enhance its analytical capability and improve its operational processes. Defined for this research effort, reference to the aforementioned DOD all source intelligence element is primarily aimed at the Defense Intelligence Agency (DIA), however, the Unified Command Joint Intelligence Centers (JICs) and specific analytic pieces of the services, such as the Air Force's National Air Intelligence Center (NAIC) and the Army's National Ground Intelligence Center (NGIC), are also part of this community.

Even before the terrible terrorist acts of September 2001, some intelligence leaders observed the global terrorist threat had evolved and changed in very complex ways, and that DOD's analytic approach had not kept pace.[2] Weakened state structures and governments, globalization in the form of informal communication, cultural, religious or business networks, and rapid technological advances allowing access to information have all contributed to expanding the power base of international terrorist groups. The typical terrorist typology represented by kidnappings, assassinations, and bombings of the 1970s and 1980s, often aimed at limited political objectives, has indeed changed.

The findings of this study are based, in part, on interviews with senior DOD Intelligence officials, congressional testimony from numerous security experts and governmental officials, and also on the works of Bruce D. Berkowitz, Allan E. Goodman, Paul R. Pillar and other scholars. The primary goal of this work is to improve DOD's capability to confront transnational terrorism. Prescriptions for the future are offered to facilitate a continuing cultural change within the DOD analytical community.

Notes

[1] The White House, *The National Security Strategy of the United States of America*, (Washington D.C., 2002), 6.

Notes

[2] Vice Adm Lowell E. Jacoby, *Information Sharing of Terrorism-Related Data*, Written Statement for the Record as part of "The Joint 9/11 Inquiry," before the Joint Hearing of the United States Senate Select Committee on Intelligence and the United States House Permanent Select Committee on Intelligence, Washington D.C., 1 October 2002, 1. On-line, Internet, 25 October 2002, Available at http://fas.org/irp/congress/2002_hr/100102jacoby.html

Chapter 2

Recognizing the Enemy: The Intelligence Community and the Terrorist Threat

It has taken almost a decade for us to comprehend the true nature of this new threat.

— President George W. Bush in *The National Security Strategy of the United States of America*, 2002

Efforts to Battle Terrorism 1993-2001: The Case Against Intelligence

To understand better the challenges transnational terrorism presents today, it is instructive to examine how the intelligence community dealt with this threat in the years preceding the September 11, 2001 attacks. Turning the calendar back to 1993, the year of the first World Trade Center (WTC) terrorist attack, we find the intelligence community grappling with change in the post-Cold War world. The primary reason for the creation of our current intelligence capability, the previous threat posed by the Soviet Union, is no longer the primary focus of the DOD. Still, despite the breakup of our former adversary and primary threat, the principal target of United States intelligence efforts remained, with good reason, state-centered threats such as Russia, North Korea, Iraq and Iran. This state-centered concentration, along with supporting a myriad of contingencies around the globe, would remain the primacy of intelligence organizations and military forces throughout the 1990s and into the new millennium. Terrorism, despite receiving an incrementally increasing focus within the overall intelligence community, would clearly play second banana.

In the aftermath of the attacks against the WTC buildings and the Pentagon, numerous critics charged that the United States intelligence team failed to recognize the significance of the changing terrorist threat. According to Richard H. Schultz and Andreas Vogt, "the real intelligence failure has to do with how the IC [sic], and the Clinton administration it served, did not understand and incorrectly assessed the transformation that terrorist organizations like al Qaeda were undergoing in the 1990s."[1] Localized terrorist organizations from the 1970s and 1980s, with their limited political agendas, had given way to a new breed of offspring with a global plan. Table 1 provides a representation of these "new terrorists," describing them as bent on mass killing, capable of operating within the borders of the United States, and focused on exploiting permissive environments such as states or territories.[2]

Table 1 Characteristics of Terrorism Emerging From Past Attacks

Terrorism Characteristics	WTC 1/ Landmarks	Khobar Towers	African Embassy	Millennium Attacks	U.S.S. Cole
Suggests new breed of terrorists seeking mass casualties emerging	X	X	X	X	
Operations in America	X			X	
Indicates al Qa'ida and like-minded individuals are particularly dangerous adversaries	X		X	X	X
Terrorists exploit sanctuary in hostile country (Afghanistan or Iran)		X	X	X	X
Terrorist exploit governments unable or unwilling to crack down, including in the west	X		X	X	

Source: Hill, Eleanor, "Hearing on the Intelligence Community's Response to Past Terrorist Attacks Against the United States from February 1993-September 2001," available at http://fas.org/irp/congress/2002_hr/100802hill.html, October 8, 2002, 9.

The more complex elements of the new terrorist breed, such as Usama bin Laden's al Qaeda network, are well organized, able to conduct long-range planning and simultaneous operations, place a heavy emphasis on operational security, have a very flexible command structure, and

exhibit skillful imagination in all facets of their operations.[3] By the late 1990s, a new generation of terrorist, distinct from standard intelligence profiles and indifferent to any concept of rational behavior, was waging war against the United States.

A second major criticism of the intelligence community was its slow reaction to the growing terrorist threat. Following the first WTC attack, a growing number of incidents and evidence indicated transnational terrorism against America was a mounting concern. In fact, a July 1995 National Intelligence Estimate recognized "a new breed of terrorist who did not have a sponsor, was loosely organized, favored an Islamic agenda, and had a penchant for violence."[4] Still, it would not be until late 1996 when the CIA and FBI dedicated specific resources and analysts to focus on the threat.[5] By this point, the intelligence community was behind the power curve in assessing global intent and depth of organization of the enemy. During this transition of the terrorist agenda in the 1990s, the Clinton administration's national security strategy confronting the enemy was principally defensive and law enforcement based. America would focus on protecting its assets and facilities abroad with defensive countermeasures, train and prepare at home to respond to contingency disasters, and as necessary, seek out the terrorist criminals and prosecute them within the United States legal system.[6] Carrying the policy over into the new millennium, the DOD and Department of State continued to focus heavily on force protection, despite the recognition, noted in a 2001 DOD report on the U.S.S. Cole attack, "that the U.S. posture in general was too defensive and that USCENTCOM is essentially operating in the midst of a terrorism war."[7]

The majority of post-September 11 retrospectives roundly condemn the Clinton administration's "law enforcement approach" to terrorism. Terrorism was viewed "as a secondary national security challenge—not a clear and present danger—even after the deadly

1998 East Africa embassy bombings. It still was not war, although the Clinton administration became somewhat more willing to go beyond the law enforcement approach and use limited cruise missile strikes against targets in Afghanistan and Sudan."[8] Clearly, some intelligence leaders recognized the growing threat terrorism presented; however, their inability to convince senior administration officials to take action beyond hunting down individual criminals or launching the occasional retaliatory military strike left the major problem intact. An organized and growing terrorist enterprise was taking hold in sanctuaries such as Afghanistan and operating freely in Africa, Europe, and even the United States itself. A prosecution mindset—focusing on the events and terrorists after the fact—blinded most to the inherent security weaknesses within our own country, permeable borders, inadequate safety measures in the transportation and other key industries, and a general public ignorance that we were, in fact, very vulnerable.

The law enforcement approach to terrorism during the 1990s, by nature of its methodology, excluded using the full capability of American military and analytical capacity. By failing to pursue a more comprehensive approach to terrorism, at least in terms of the military instrument of power, a major obstacle to combating terrorism was essentially masked--the poor coordination and lack or interoperability within the overall intelligence community. This topic is addressed more in-depth later, but its recognition as perhaps the most important failing of intelligence prior to September 11, as well as today, is important. The inability of DOD, CIA, the Department of State, the FBI, and others to coordinate effectively and really understand each other's worlds was, and still is, a major impediment to progress. An example of the differing worlds is illustrated by the case of Usama bin Laden operatives Khalid al-Mihdhar and Nawaf al Hazmi. Evidence from open congressional hearings suggests information concerning these two individual's plans to acquire visas and travel to the United States was not passed from the CIA to

the FBI in anything resembling a timely manner, despite numerous opportunities to do so between January 2000 and June 2001.[9] The pair was eventually watch-listed by the CIA in August 2001, and the FBI was notified of their likely presence in the United States.[10] This example is not meant to single out the CIA. Other well-documented examples of intelligence coordination shortcomings also exist. Notwithstanding the seriousness of these lapses, one should not blindly point to organizational arrogance or spiteful intentions as causing the gap in coordination between the aforementioned agencies. It is more likely a simple cultural failing; coming from different worlds, each agency really did not appreciate the needs of the other in the intensifying battle against terrorism.[11]

Efforts to Battle Terrorism 1993-2001: The Case for Intelligence

Turning the coin over, many of the arguments condemning the intelligence community's performance prior to September 11 can be viewed from another perspective. The policy of the Clinton administration in the 1990s was that terrorism was neither a level-one national security challenge nor a form of warfare.[12] Those who saw it as such, when the world was faced with rogue states, innumerable contingency operations and nuclear weapons proliferation, were demeaned as naïve and even extreme.[13] The message most in the national security community espoused, despite several attacks against American facilities and personnel overseas, was that "prior to the 11 September attacks, terrorist operations against United States' interests were not seen as posing a grave threat to the national security of the United States."[14] The idea of going to war with al Qaeda, unleashing the full power of the United States military, and dedicating the priority of American intelligence resources, was not in the forefront of American national security thinking.

This assertion is advanced by the distribution of responsibilities to confront terrorism by the Clinton administration, and prior to September 11th, the Bush administration. Presidential Decision Directive-39, signed by President Clinton in 1995, assigned responsibility for counterterrorism policy and operations abroad to the Department of State.[15] This same directive further designated the Department of Justice as lead agency for domestic terrorism.[16] Further, early in the current Bush administration, the new director of the Federal Emergency Management Agency (FEMA) was successful in obtaining a presidential directive identifying catastrophic terrorism as a disaster vice a crime or war, and had this responsibility added under the responsibility of his agency.[17] Therefore, although terrorism was high on the agendas of both the Clinton and Bush administrations, it was clearly under the guise of diplomatic policy, criminal prosecution or disaster response. It was not at the very top echelon of national security priorities, in spite of the growing threat being espoused by many in the Intelligence Community.

The weight of evidence available today clearly bears out the leadership of the Intelligence Community took the threat of transnational terrorism very seriously well before the tragic events of September 2001. For many years, pockets or cells of analysts within DOD, CIA and other agencies have been focused on the terrorist threat in some manner or another. This effort increased accordingly in the past six or seven years to meet the rise of the growing terrorist threat espoused by numerous intelligence leaders. For example, in 1996, after several years of monitoring activity in the Sudan, the CIA formulated a specific bin Laden Issue Station team for tracking the al Qaeda terrorist cell.[18] A short time later, in December 1998, the Director of Central Intelligence (DCI) went one step further declaring war on Usama bin Laden, pledging the full weight of the intelligence community's effort in this endeavor.[19] In March 2001, DIA Director Vice Admiral Thomas R. Wilson, echoed testimony from previous years and previous

directors when he told Congress one of his gravest concerns is "a major terrorist attack against United States interests, either here or abroad, perhaps with a weapon designed to produce mass casualties. Terrorism remains the 'asymmetric approach of choice' and many terrorist groups have both the capability and desire to harm us. Terrorism is the most likely direct threat to US [sic] interests worldwide."[20] Not only did the intelligence community recognize the seriousness of the new global threat, it was very much engaged in battling terrorism, and to the credit of many, achieved numerous successes in thwarting potential attacks. As Richard Betts notes,

> Contrary to the image left by the destruction of September 11, U.S. intelligence and associated services have generally done very well at protecting the country. In the aftermath of a catastrophe, great successes in thwarting previous terrorist attacks are too easily forgotten—successes such as the foiling of plots to bomb New York City's Lincoln and Holland tunnels in 1993, to bring down 11 American airliners in Asia in 1995, to mount attacks around the millennium on the West Coast and in Jordan, and to strike U.S. forces in the Middle East in the summer of 2001.[21]

The case supporting intelligence only gets stronger when one looks at the repeated warnings offered by senior intelligence officials, outside experts, various commissions and Congress regarding the severity of the terrorist threat.

In recent testimony before Congress on the Intelligence Community's performance to combat terrorism from 1993 to 2001, Eleanor Hill, Staff Director, the Joint Inquiry Staff observed, "this change in lethality was recognized early on within the Intelligence Community and by outside experts and communicated to U.S. government policymakers. The DCI's December 1998 declaration of war on al-Qa'ida [sic] is only one indication of how seriously the danger of terrorism was taken within the Community [sic]. Policymakers from the Clinton and Bush administration have testified that the Intelligence Community repeatedly warned them of the danger al-Qa'ida [sic] posed and the urgency of the threat."[22] Moreover, between 1998 and 2000, Congress alone held over 80 sessions on terrorism, involving a wide range of

committees.[23] They also chartered numerous commissions to study the various aspects of the terrorist threat and American domestic response capabilities, the two most notable being the Hart-Rudman commission named for its co-chairs, former Senators Gary Hart and Warren Rudman and the Gilmore Commission named for its chair, former Virginia Governor, James Gilmore III. The Hart-Rudman study concluded that attacks against the American homeland were likely over the next quarter century and urged the United States Government to make homeland security its primary national security mission.[24] The Gilmore Commission provided similar findings calling upon the federal government to develop a workable strategy on national domestic preparedness plans to combat terrorism.[25] The Gilmore Commission also chastised the legislative and executive branches for their inadequate progress in battling terrorism, highlighting numerous failed attempts to coordinate a cohesive government terrorism program and noting more than two dozen congressional committees having some responsibility for terrorism programs.[26]

The key contributions of studies such as Hart-Rudman and Gilmore Commissions were not necessarily their confirmation of the threat or recommendations to prepare for catastrophic terrorist attacks, but their identification of a key problem facing the intelligence community and other government agencies--the lack of a coherent and focused national strategy on terrorism. According to the Gilmore Commission report,

> The lack of a national strategy results in part from the fragmentation of Executive Branch programs for combating terrorism. These programs cross an extraordinary number of jurisdictions and substantive domains: national security, law enforcement, intelligence, emergency management, fire protection, public health, medical care, as well as parts of the private sector. No one, at any level, is ``in charge'' of all relevant capabilities, most of which are not dedicated exclusively to combating terrorism. The lack of a national strategy is inextricably linked to the fact that no entity has the authority to direct all of the entities that may be engaged. At the Federal level, no entity has the authority even to direct the coordination of relevant Federal efforts.[27]

That a much more cohesive approach to terrorism was required across the federal government was recognized early on within the Intelligence Community. In February 1998, former Director of Central Intelligence Mr. James Woolsey told Congress "the risk that terrorists may use weapons of mass destruction constitutes, in my view, the number one threat to our national security…There is no silver bullet that will stop terrorism, but there is a major need for a thorough and coordinated approach to the problem that I believe is still lacking in the U.S. Government."[28] It was painfully clear to many observers that although the gravity of the terrorist threat was well recognized at the end of the twentieth century, the United States government was either unable or unwilling to take the steps necessary to confront the enemy head-on. Perhaps governmental and bureaucratic changes like we are seeing now are just unfathomable without a precipitous event like September 11. Maybe public opinion or sentiment would not have supported increased resources and security precautions because the true depth of the threat was not really known or advertised. Whatever the case, the strategic direction and resources necessary to vector the Intelligence Community and make terrorism a top tier national priority were not forthcoming before September 11.

Presidential Decision Directive-35 (PDD-35) set the Intelligence Community's strategic-level guidance for national security priorities beginning in 1995.[29] Using a broad-based tier system, which would be reevaluated and updated annually, PDD-35's goal was to rank the myriad of post-Cold War threats facing the United States.[30] Unfortunately, PDD-35 was never amended, and as certain threats, including terrorism, increased in the late 1990s, none of the lower-level priorities were downgraded so that resources could be reallocated.[31] The problem was simple; everything was a priority so nothing ever slipped off the plate of the intelligence professional. To the contrary, as resources fell following the dissolution of the former Soviet

Union, a rapid increase in contingency operations and military deployments actually drove up many intelligence requirements. Unfortunately, according to Director of Central Intelligence, Mr. George Tenet, "the cost of the 'peace dividend' was that during the 1990s our Intelligence Community funding declined in real terms--reducing our buying power by tens of billions of dollars over the decade. We lost nearly one in four of our positions. This loss of manpower was devastating, particularly in our two most manpower intensive activities: all-source analysis and human source collection."[32] In the face of declining overall resources, the Intelligence Community was forced to make difficult trade-offs internally to ensure counterterrorist efforts matched the growing threat. A representative example of this is the 50 percent increase within CIA funding levels for counterterrorism just prior to September 11 when compared against funding for the program in fiscal year 1997 expenditures.[33]

One can find merit in arguments either condemning or defending the Intelligence Community's performance prior to the September 11th terrorist attacks. The crucial point for this study is where we are headed now that most everyone in the national security apparatus recognizes the full extent of the transnational terrorist threat. To this end, and with specific reference to, or impact on, the DOD analytic community, it is essential to identify existing intelligence gaps and key lessons learned from the September 2001 attacks.

Notes

[1] Richard H. Schultz and Andreas Vogt, "The Real Intelligence Failure on 9/11 and the Case for a Doctrine of Striking First," in *Terrorism and Counterterrorism: Understanding the New Security Environment*, ed. Russell D. Howard and Reid L. Sawyer (Guilford, Connecticut: McGraw-Hill/Dushkin, 2002), 368.

[2] Eleanor Hill, *Intelligence Community's Response to Past Terrorist Attacks Against the United States from February 1993-September 2001*, Statement before the Joint Hearing of the United States Senate Select Committee on Intelligence and the United States House Permanent Select Committee on Intelligence, Washington D.C., 8 October 2002, 9., On-line, Internet, 25 October 2002, Available at http://fas.org/irp/congress/2002_hr/100802hill.html.

[3] Ibid., 9-10.

Notes

[4] Ibid, 9.

[5] Ibid.

[6] The White House, *A National Security Strategy for a Golden Age*, (Washington, D.C., 2000), 1-7.

[7] Hill, *Response to Past Terrorist Attacks*, 1.

[8] Shultz, 370.

[9] Eleanor Hill, *Joint Inquiry Staff Statement*, Statement before the Joint Hearing of the United States Senate Select Committee on Intelligence and the United States House Permanent Select Committee on Intelligence, Washington D.C., 17 October 2002, NP., On-line, 25 October 2002, Available at http://fas.org/irp/congress/2002_hr/101702hill.html.

[10] Ibid, NP.

[11] Mr. Louis Andre, Senior Civilian Advisor to the Director, Defense Intelligence Agency, interview by author, 18 December 2002, Washington D.C., notes.

[12] Schultz, 384.

[13] Ibid.

[14] Vice Adm Lowell E. Jacoby, *DIA Response to Joint 9/11 Letter of Invitation*, Written Statement for the record as part of "The Joint 9/11 Inquiry," before the Joint Hearing of the United States Senate Select Committee on Intelligence and the United States House Permanent Select Committee on Intelligence, Washington D.C., 17 October 2002, 2., On-line, Internet, 25 October 2002, Available at http://fas.org/irp/congress/2002_hr/101702jacoby.html.

[15] Ambassador Philip C. Wilcox Jr., *Combating International Terrorism*, Statement for the record before the House Permanent Select Committee on Intelligence, 5 March 1996, 1. On-line, Internet, 25 October 2002, Available at http://fas.org/irp/congress/1996_hr/h960305w.html.

[16] Ibid., 1.

[17] Ashton B. Carter, "The Architecture of Government in the Face of Terrorism," in *Terrorism and Counterterrorism: Understanding the New Security Environment*, ed. Russell D. Howard and Reid L. Sawyer (Guilford, Connecticut: McGraw-Hill/Dushkin, 2002), 430.

[18] Hill, *Joint Inquiry Staff Statement*, NP.

[19] Ibid., NP.

[20] Vice Adm Thomas R. Wilson, *Global Threats and Challenges Through 2015*, Statement for the Record before the United States Senate Armed Services Committee, 8 March 2001, NP., On-line, Internet, 25 October 2002, Available at http://fas.org/irp/congress/2001_hr/s010308w.html.

[21] Betts, 473.

[22] Hill, *Response to Past Terrorist Attacks*, 9.

[23] Laura K. Donohue, "Counterterrorism, Individual Rights, and U.S. Foreign Relations Post 9-11," in Terrorism and Counterterrorism: Understanding the New Security Environment, ed. Russell D. Howard and Reid L. Sawyer (Guilford, Connecticut: McGraw-Hill/Dushkin, 2002), 277.

[24] Senate, The Committee on Foreign Relations, *Strategies for Homeland Defense: A Compilation by the Committee on Foreign Relations*, 107th Congress, 1st sess., (Washington D.C.: GPO, 2001), NP.

[25] Ibid., NP.

[26] Ibid., NP.

Notes

[27] Ibid., NP.

[28] Mr. James R. Woolsey, Statement for the Record before the United States House or Representatives Committee on National Security, 12 February 1998, NP., On-line, Internet, 25 October 2002, Available at http://fas.org/irp/congress/1998_hr/h9800212.html.

[29] Hill, *Response to Past Terrorist Attacks*, 21.

[30] Ibid.

[31] Ibid.

[32] Mr. George Tenet, Written Statement for the record as part of "The Joint 9/11 Inquiry," before the Joint Hearing of the United States Senate Select Committee on Intelligence and the United States House Permanent Select Committee on Intelligence, Washington D.C., 17 October 2002, 16-17., On-line, Internet, 25 October 2002, Available at http://fas.org/irp/congress/2002_hr/101702tenet.html.

[33] Ibid., 23.

Chapter 3

Intelligence Gaps and Lessons Learned

To support preemptive options, we will: build better, more integrated intelligence capabilities to provide timely, accurate information on threats, wherever they may emerge.

—President George W. Bush in *The National Security Strategy of the United States of America*, 2002

Many post September 11 assessments of the Intelligence Community, including congressional testimony from senior government officials, defense experts and community insiders, acknowledge resources for intelligence had been cut too deeply during the 1990s.[1] Among the most prominent lessons learned for the DOD intelligence apparatus is an under investment in human intelligence (HUMINT) and analytic expertise. Continual cutbacks, yearly resource shortfalls, a lack of investment in recruiting and sustainment, and an apparent reluctance at the policy level to recognize the value of HUMINT operations all resulted in a degraded situation for the DOD Intelligence Community.[2] The most obvious setback resulting from the lack of investment in HUMINT is the inability to collect on the shadowy, secretive individuals making up the terrorist target set. Expanding the depth and breadth of information upon which an analytic capability can be based is critically dependent on a robust HUMINT capability. Unfortunately, fixing this gap cannot be done quickly, easily, or through quick infusions of money.[3] Recovering from deep manpower reductions, and reconstituting the cadre of seasoned case officers and assets overseas, will likely take many years.[4]

An equally debilitating shortfall within DOD is the lack of trained all-source intelligence analysts. The sheer numbers of individuals necessary to process and assess the flood of information related to terrorism is staggering. As Congressman Porter Goss noted recently in an interview with the Brookings Institute, "we don't have enough analysts. We are hopelessly under invested in analysts. These are again, the language people, the people familiar with the culture, the people who have actually been on the street in Khartoum or wherever you want to go, who understand a little bit what this means."[5] Increasing the number of analysts to study terrorism is not the only problem however. We must build a robust pool of experts who recognize the changing enemy and can understand their motives and modes of operation. Benign activities from yesteryear; stealing identification cards, purchasing plane tickets with cash, suspicious activity noted by a local citizens to mention but a few, must now be taken into account by intelligence analysts[6]. According to current DIA Director Admiral Jacoby,

> We were surprised analytically by the complexity of the overall plan, the stunning simplicity of "weaponizing" for mass casualties, and the benign backgrounds of the individual attackers. Our underlying assumptions about bin Ladin's creativity and limits on his actions were wrong. In short, long-held analytic assumptions about terrorist groups and their intentions, values, constraints, and methods of operation—which were challenged by the earlier attack on the USS COLE—were completely shattered on 11 September.[7]

The simple and brutal lesson for all of America is we're vulnerable as a society. The makeup and focus of the twenty-first century terrorist enemy has truly changed. With a growing emphasis on near-term threat warning, building and sustaining a skillful analytic capability to address this renewed threat is a mounting challenge for DOD.

Struggling to keep pace with advancing technology is a seemingly ever-present growing intelligence gap. Maintaining the ability to collect, process, and analyze intelligence information in a timely manner is often a daily struggle and a lesson learned from numerous past conflicts.

Within DOD, upgrades across many sectors are required to ensure the United States does not completely lose the ability to collect and utilize intelligence against techno-savvy terrorists.[8] Equally important, is ensuring our principal customer, military combatants, have access to timely intelligence information in a usable format.[9] Again, this is best achieved through investment in development and maintenance of leading-edge communications and information technology systems. With success in counterterrorist operations sometimes measured in hours or minutes, meeting the technological challenges offered by changing target priorities, dynamic communications links, and the like, are more and more relevant with each passing day. Supporting an increased investment in tools and systems to help the analyst, investing in relational database software and focused systems development, and embracing expanded communications bandwidth and link analysis technology, is imperative for future success.

Resource and technological gaps notwithstanding, several key lessons learned as a result of the September 11 attacks are procedural, cultural, or policy based. In hindsight key policy decisions or restrictions have had significant influence in our ability to combat transnational terrorism. For example as late as the year 2000, the Clinton administration stressed the need to devote the necessary resources for America's strategy to combat terrorism; however, the focus was still on a graduated scale of intelligence gathering and enhanced law enforcement.[10] Since September 11, the emerging Bush doctrine has begun changing a "U.S. government mindset and two-decade old defensive counterterrorism policy from conceding the initiative to the terrorists to seizing the initiative by striking first through offensive military operations."[11] Spurred by the passage of the USA-Patriot Act of 2001, several major policy changes have begun clearing some of the bureaucratic hurdles. Three especially vital changes include: making information collected by law enforcement agencies, including grand jury testimony, available to intelligence

agencies;[12] rolling back the guidelines adopted in 1995 restricting recruitment of unsavory sources or agents by the Intelligence Community;[13] and the decision to aggressively pursue military action in previously off limits terrorist sanctuaries such as Afghanistan where mastermind Usama bin Laden organized, trained, and grew his al Qaeda network into a world-wide menace.[14] Each of these policy changes has spurred some controversy in their own right with the decision to make grand jury testimony available to intelligence agencies receiving the most attention. Debates concerning the long-term impacts of the grand jury testimony decision on individual civil liberties continue and are beyond the scope of this paper, however, one critical point is worth mentioning in this regard. The realization the United States is in a new type of fight against an organized and formidable enemy, and new sacrifices by both the government and American public must be made if we are to successfully combat this threat, has at least been reached by many. Yet, despite advances such as those mentioned above, further progress within DOD is necessary to bring focus on the terrorist effort. As we enter the year 2003, fully 29 separate organizations within DOD still share some part of the terrorist pie, and another 11 organizations play some role in the counter-intelligence realm.[15] Obviously, some level of consolidation of responsibilities or focus must occur to improve coordination and information sharing.

The biggest lesson learned from the September 11 attacks, according to the majority of senior DOD intelligence officials interviewed for this paper, is our continued inability to efficiently access and share timely intelligence information within DOD and the larger Intelligence Community as a whole.[16] This limitation has impacted both DOD's ability to conduct all-source analysis and its ability to respond effectively to changing indications and warning (I&W) requirements. Responding to questions about information sharing, DIA Director

Admiral Jacoby told the Joint Congressional Inquiry on September 11, "DIA does not have access to all intelligence and law enforcement information on terrorists…I believe the un-shared information falls largely into the categories of background or contextual data, sourcing, seemingly benign activities, and the like. But, as previously mentioned, it is within these categories that the critical 'connecting dot' may well be found."[17] Again, the underlying cause for this problem is not ostensibly talent based, approach based, or even rigid spitefulness, but cultural. Some of the approaches seemingly necessary to address transnational terrorism effectively—in-depth, daily coordination across agencies; increased information sharing; and common databases and communication environments—are arguably foreign concepts with respect to bringing together the law enforcement and intelligence communities built over the last fifty-plus years.

The biggest cultural gap in information sharing, somewhat understandably, is between the law enforcement agencies and intelligence world focused on the foreign threat. The FBI's traditional focus is domestic law and security and involves a process that is criminally based, evidence bound, and concerned with investigation rather than speculation or analysis. Like many of its intelligence community brothers, the FBI is insulated in much of what it does and is not used to sharing information it owns or has collected. Former Director of Central Intelligence John Deutch, and former chief legal counsel at CIA, Mr. Jeffery Smith, offer an example of the two clashing worlds.

> Law enforcement's focus is to collect evidence after a crime is committed in order to support prosecution in a court of law. The FBI is reluctant to share with other government agencies the information obtained from its informants for fear of compromising future court action. On the other hand, the CIA collects and analyzes information in order to forewarn the government before an act occurs. The CIA is reluctant to give the FBI information obtained from CIA agents for fear that its sources and methods for gaining that information will be revealed in court.[18]

The most disconcerting cultural gap, however, is witnessed by the lack of coordination and information sharing within the traditional Intelligence Community itself. The quest for sharing opportunities, new information technologies, enhanced data mining techniques, and more dynamic databases is underway; however, compromise remains a valid, major concern.[19] The DOD intelligence apparatus is simply caught in the intelligence professional's age old catch-22; the endeavor of effectively sharing timely information without bringing undue risk to critical information sources and methods. Still, a concession or happy medium between these competing priorities must be reached or the Intelligence Community will continue to struggle with its current information stovepipes and "lag behind the private sector in its ability to tag and store massive amounts of data, and to mine that information to determine patterns. Again, a culture that discourages collaboration and the sharing of information forfeits these new technological advantages."[20]

Notes

[1] Honorable Paul Wolfowitz, Prepared Statement for the record as part of *The Joint Inquiry on Counterterrorist Center Customer Perspective*, before the Joint Hearing of the United States Senate Select Committee on Intelligence and the United States House Permanent Select Committee on Intelligence, Washington D.C., 19 September 2002, 2. On-line, Internet, 25 October 2002, Available at http://fas.org/irp/congress/2002_hr/091902wolfowitz.html.

[2] Lt Gen (Retired) Patrick M. Hughes, Prepared testimony before the United States Senate Committee on Governmental Affairs, 26 June 2002, NP. On-line, Internet, 25 October 2002, Available at http://fas.org/irp/congress/2002_hr/062602hughes.html.

[3] Richard K. Betts Jr., "Fixing Intelligence," in *Terrorism and Counterterrorism: Understanding the New Security Environment*, ed. Russell D. Howard and Reid L. Sawyer (Guilford, Connecticut: McGraw-Hill/Dushkin, 2002), 475.

[4] Tenet, 24.

[5] Congressman Porter Goss, "The Need for Human Intelligence," a PBS Frontline Interview, 2001, NP., On-line, Internet, 25 October 2002 Available at http://www.pbs.org/wgbh/pages/frontline/shows/terrorism/fail/why.html.

[6] Andre, 18 Dec 2002 Interview, NP.

[7] Jacoby, *DIA Response to 9/11*, 2.

Notes

[8] Ambassador Paul L. Bremer III, *National Commission on Terrorism*, Testimony before the United States Senate Select Committee on Intelligence, 8 June 2000, NP., On-line, Internet, 25 Oct 2002, Available at http://fas.org/irp/congress/2000_hr/000608_bremer_terrorism.html.

[9] Vice Adm Thomas R. Wilson, *Global Threats and Challenges Through 2015*, Statement for the Record before the United States Senate Armed Services Committee, 19 March 2002, 27., On-line, Internet, 25 October 2002, Available at http://fas.org/irp/congress/2002_hr/031902.pdf.

[10] The White House, *A National Security Strategy*, 2001, 1-7.

[11] Shultz, 368.

[12] Richard A. Best Jr., *Intelligence to Counter Terrorism: Issues for Congress*, (Washington D.C., Congressional Research Service, *The Library of Congress*, 2002), 16., On-line, Internet, 25 October 2002, Available at http://www.fas.org/irp/crs/RL31292.pdf.

[13] United States Congress, *Strategies for Homeland Defense*, NP.

[14] Hill, *Response to Past Terrorist Attacks*, 5.

[15] Col Jon Wohlman, Chief, Intelligence Plans and Programs, Joint Chiefs of Staff, interview by author, 18 December 2002, Washington D.C., notes.

[16] Mr. Pat Deucy, Chief, Joint Interagency Task Force—Counterterrorism, DIA, interview by author, 17 December 2002, Washington D.C., notes.

[17] Jacoby, *Sharing of Terrorism-Related Data*, 5.

[18] John Deutch and Jeffrey H. Smith, "Smarter Intelligence," *Foreign Policy Magazine*, January 2002, NP. On-line, Internet, 25 October 2002, Available at http://www.foreignpolicy.com/issue_janfeb_2002/deutch.html.

[19] Rear Admiral Murret, Deputy Director for Intelligence, Joint Chiefs of Staff, interview by author, 17 December 2002, Washington D.C., notes.

[20] Wolfowitz, *Counterterrorist Center Customer Perspective*, 6.

Chapter 4

Changing the Cultural Mindset

> *A fate that can befall a bureaucracy that does not keep up is to muddle along until a catastrophe exposes the organization's unseen weakness. One can imagine how such a catastrophe might occur for the intelligence community today. It would likely be a threat that is totally off the radar screen now, but which—as was the case with the Iranian revolution—results in large costs that directly affect the American public.*
>
> — Bruce D. Berkowitz and Allan E. Goodman in
> *Best Truth: Intelligence in the Information Age*, 2000

DOD intelligence professionals are committed to providing the best possible intelligence support for United States military forces and decision makers. Broadly brushed, this analytical support is typically concerned with the decisions and intent of foreign leaders and military commanders; revolves around identifying enemy state orders of battle and operational doctrine; encompasses traditional roles such as targeting, indications and warning, and near-real-time reporting of changing events; and most importantly, is focused on transmitting accurate and timely intelligence to our own military commanders. Of course, this brief description is a gross over-simplification of the world of intelligence operations; the key point being the primary focus of DOD intelligence analysis prior to September 11, 2001 was on the foreign state and its associated military weaponry and forces. The rise of transnational terrorism as a central concern for national security policy does not mean the traditional state threat or the rest of the world disappears from the horizon. In fact, as Secretary of Defense Donald Rumsfeld expressed in a

recent National Defense University speech, "we cannot and must not make the mistake, of assuming that terrorism is the only threat. The next threat we face may indeed be against terrorists–but it could also be a cyber-war, a traditional, state-on-state war...or something entirely different."[1]

Alternatively, dealing with the complexities and analytic challenges posed by twenty-first century terrorism is a daunting task for DOD. For the past 50 years, our intelligence effort has concentrated on defeating external, nation-state threats. It is now clear we must apply the same level of effort to non-state actors and threats emanating from within our own borders.[2] Former CIA General Counsel, Jeffery Smith, identified the difficulties of the task when he said,

> Dealing with these groups is much, much more difficult. They are, as often said, para-statal [sic]; they're not a government; they're not a state; but they have many of the attributes of a state. They're big, they're well financed, they're secretive, they operate outside of ordinary established legal channels. They enjoy support across a number of governments. We don't have formal relations with them like we did with the Soviet Union. We don't have a series of back channels with them like we did with the Soviet Union, and they don't behave in a responsible fashion like, at the end of the day, the Soviets did, with respect to managing their nuclear weapons. It's a fundamentally different situation and we're going to have to look at the way we conduct our business, at the way we confront it, and at the way we fight it.[3]

At the most basic level, the terrorist threat brings with it the challenge of confronting the technologically empowered group or individual; an enemy difficult to find, track, and one who is not necessarily bound by bureaucratic decision cycles. Clearly, state-oriented threat approaches are, by themselves, insufficient to cover the transnational threat spectrum existing today. Globalization is creating a new environment that transcends international borders and minimizes the importance of traditional boundaries. Small cells operating within a state, or larger networks operating worldwide have proven they can do the United States great harm.[4] Taken a step further, some scholars argue terrorist groups are now competing with States for international

attention and power. Advances in technology have allowed small groups to impact the international system through a simultaneous diffusion of knowledge and capability.[5] Large-scale terrorist attacks in Nigeria, the United States and most recently Indonesia, where the sovereign state is seemingly unable to guarantee the safety of its populace, provides the latest evidence supporting this argument. Perhaps Martin Van Creveld's assertion from twelve years ago is coming to fruition, "as war between states exits through one side of history's revolving door, low intensity conflict among different organizations will enter through the other…national sovereignties are being undermined by organizations that refuse to recognize the state's monopoly over armed violence."[6]

The expanding and changing global terrorist threat adds a new and different dimension to the plate of the intelligence professional, one that requires an altering of traditional intelligence culture to successfully address. When looking at organizational culture, a key feature is that members "share values, practices, and beliefs, in addition to a common set of assumptions about how the world works. This encourages predictability and stability."[7] Predictability and stability are qualities cherished within intelligence organizations, a community which, due to the nature of its business, is rooted in closed doors, secrecy, compartmentalization, and in-depth knowledge. These attributes are unquestionably necessary pieces of the intelligence world and have served the United States well against the monolithic state enemies of the last fifty-plus years. At the same time, excessive secrecy, assumed knowledge and expertise and disproportionate compartmentalization can also be roadblocks to battling effectively the global and fluid terrorist enemy. Granted, some analysts and organizational elements within DIA or CIA, for example, have developed superb capabilities and processes in the battle against terrorism. However, within the larger DOD analytic community, and the greater Intelligence

Community as a whole, a culture that does not share information well and does not understand the roles and needs of sister intelligence organizations, persists. The natural concern emanating from this mindset is that it may keep us from "replacing practices that are inefficient, out of date, or simply wrong."[8] The traditional concepts of smothering secrecy and compartmentalization, and expected knowledge as a result of that secrecy, must be examined closely if we are to combat terrorism successfully abroad and at home.

The visions of secrecy and knowledge are associated with the business of intelligence, perhaps like no others. History is filled with tales of swashbuckling intelligence personalities and successful secretive intelligence operations. History is equally replete with stories regarding the price paid by societies for failing to keep, or unearth, important intelligence secrets. Essentially, these cultural attributes define how intelligence specialists see themselves and how the rest of society sees the intelligence community.[9] Secrecy and security are especially vital parts of the intelligence business and will always be so. Protection of sources and methods is the key foundational element for any intelligence program and an indispensable piece for successful operations. For the most part, most Americans understand this and agree that the government needs to keep many intelligence activities secret.[10] Some critics argue, however, the problem with the Intelligence Community culture is that too often, secrecy is the default option.[11] Undoubtedly, when confronting terrorist networks like al Qaeda, faster and more aggressive measures for sharing information must be found. Addressing the Joint Congressional Inquiry investigating September 11, Admiral Jacoby declared, "I recognize and accept that some information cannot be fully shared. But, what can be shared must be shared."[12]

Noticeably, the biggest drawback surrounding the culture where secrecy prevails is the impact on information sharing and access. "Cold War intelligence lived in a world where

information was scarce; it relied on 'secrets' not otherwise available. Its business was those secrets. Now, though, it faces an era of information. Information and its sources are mushrooming, and so are the technologies for moving information rapidly around the globe."[13] Translated to the war against terrorism, valuable information now exists outside of the state sheltered defense apparatus and may be found from such non-traditional intelligence sources as the Internet, university professors, local police forces, or state immigration services to mention but a few. The DOD Intelligence Community must learn to acquire intelligence by methods markedly different from those to which they are accustomed.[14] The target is no longer a just place on the ground. It is now the individual terrorist or terrorist group and the lines differentiating the DOD intelligence community from the FBI's traditional law enforcement world are ever blurring. Given these conditions, many argue the business of intelligence is no longer just about secrets, its business now is to provide a far-reaching understanding of the world using all available sources.[15] Understanding the multifaceted challenges presented by terrorism, the predominant culture of secrecy must be studied to ensure DOD makes the most of new technology and adapts to how its customers want to access, and use, information.[16]

Knowledge is closely related to secrecy in that intelligence professionals, by nature of their occupation and access to secrets, are viewed by the public as "providing judgments that are, at least on some subjects, better than those they can find elsewhere."[17] Obviously, this perception is also held by intelligence professionals and is an ingrained part of the intelligence culture. There are many good reasons for the aforementioned generalization, not least of which is the assumption the intelligence professional "knows best" is correct the vast majority of the time. The average intelligence analyst spends the preponderance of his or her career developing in-depth knowledge about a region, country, culture or enemy military force—they are experts.

The concern arises for some, especially with regard to transnational terrorism, when it is assumed all knowledge comes from secrets and is held by the intelligence analysts only. Critics charge the DOD Intelligence Community is "unable to address increasingly diverse constituencies, to exploit the growth in open-source intelligence or to harness the technical skills available in the private sector. The long-term investments in education and research capabilities necessary to provide national pools of political, strategic, and technical expertise from which the intelligence agencies can draw remain undefined and unfounded."[18] In the battle against terrorism, it is critical the DOD Intelligence Community aggressively pursue a philosophy using all available resources of knowledge and expertise. This is especially important during the pre-incident period where potential terrorist activities are more likely observed by ordinary citizens, local business security forces, or by police than by traditional intelligence collectors.[19]

Secrecy and knowledge notwithstanding, the biggest cultural barrier the DOD Intelligence Community faces today is compartmentalization. For the purposes of this study, compartmentalization is defined as the inability or unwillingness to share data within the Intelligence Community itself. This obstacle has many roots or origins: the segmenting of information within various organizations due to classification; having differing technological capabilities between organizations; operating on different networks or systems; or just simply not being willing to share intelligence information for fear of compromise, to mention but a few. Many of these rationales are valid concerns and necessary processes, while others are less well founded, entrenched in bureaucracy or culture. The terrible events of September 11 served as a catalyst to begin addressing the intelligence business' compartmentalization culture; however, much remains to be done. In addressing the topic of information sharing of terrorism-related data before Congress recently, then Acting DIA Director Admiral Jacoby observed,

> Historically, we've had mixed results regarding the effectiveness of community partnerships. The mere act of assigning an analyst to another organization does not ensure a greater level of access to information or more open sharing of information. JITF-CT analysts in counterpart organizations do not have unfettered and unconditional access to all relevant terrorist information. By virtue of their status, these analysts are unquestionably afforded greater access to host-agency data; but, in some cases, they are restricted from making that additional information available to colleagues at their home agency. As such, some of the tangible benefits and explicit objectives of exchanging personnel—sharing of information and leveraging collective expertise—are degraded. However, real progress has been made in the past year and I am optimistic that the full benefits and objectives of community integration will ultimately be realized.[20]

Before any true community integration can occur, the problem of excessive compartmentalization must be addressed. Two issues impeding this integration are, for lack of better terminology, mission transition and ownership of data.

Issues with mission transition are best witnessed in the FBI and its ongoing partnership with the foreign intelligence organizations. The FBI itself recognizes it is far behind the CIA and DOD Intelligence Community in its hi-tech capabilities to process and store data.[21] Perhaps due to lingering sensitivities concerning evidence protection, the FBI still prints all of its information cables hardcopy, maintains no centralized digital repository for analytical information and has no existing mechanism to interface with similar DOD systems.[22] Moreover, the philosophical mindset of the FBI is still investigative or after-the-fact, rather than speculative or pre-emptive.[23] Given the small footprint of terrorist organizations, their remarkable efforts to conceal operations, and the likelihood much of their benign indicators will escape traditional intelligence collectors, a cohesive and integrated effort between the FBI and the DOD intelligence apparatus is paramount. The Law Enforcement Community must transition to an analytical approach as well as an investigative mindset, and DOD analysts must have more timely access to law enforcement data on individual terrorist and terrorist groups.

The ‘ownership of data’ paradigm must also be addressed for DOD to effectively deal with the convoluted nature of global terrorism.[24] This issue basically translates to the understanding that an organization that collects the data owns it, and the collecting organization will decide what it can, or will, share with other organizations. As previously stated in this paper, certain sensitive information must always be protected. The problem caused by overzealous ownership is too often security caveats preclude inclusion of reports in large electronic databases where link analysis technology and other analytic tools can be applied. Per Admiral Jacoby, “I remain steadfast in my belief—elaborated upon in previous statements—that the analytic component of the Intelligence Community can make a greater contribution to the war on terrorism if given access to a much wider range of information and supported with more capable technologic tools.”[25]

Compartmentalization’s impact is most clearly felt in the areas of timeliness and analysis. Timely sharing of data or simultaneously referencing the same data only enhances the quality of intelligence. Consequently, especially with regard to supporting military forces, the DOD must stress networking, speed of exchange, and access to information for people who need it, whenever and wherever they need it.[26] Still, tactical warning in the fight against terrorism is rare and will continue to be the “holy grail” for intelligence professionals and law enforcement officials. Former Senator Warren Rudman, commenting in an interview following the September 11 attacks, offered a colorful yet unnerving appraisal: “anybody who believes that intelligence, even with beefing up human intelligence, will be good enough to predict that these shadowy organizations can be penetrated in a way that we will be able to, with impunity, determine what they're going to do and where and when they're going to do it -- they're just whistling in the cemetery. That is not going to happen.”[27] Yet, despite the monumental

complexities of this task, timely, precise, and actionable intelligence is among the most important tools in the fight against terrorism. Increasing the DOD Intelligence Community's contribution to this effort will rely heavily on skillful and creative analysis and access to all available data.

Notes

[1]Best, *Intelligence to Counterterrorism*, 21.

[2] Wolfowitz, *Counterterrorist Center Customer Perspective*, 3-4.

[3] Jeffrey Smith, "Constraints and Obstacles Facing U.S. Intelligence," Excerpts from a PBS Frontline Interview, 2001, NP., On-line, Internet, 25 October 2002, Available at http://www.pbs.org/wgbh/pages/frontline/shows/terrorism/fail/constraints.html.

[4] Wilson, "Global Threats and Challenges 2002," 19.

[5] Notes, U.S. National Security lecture by Professor Mohiaddin Mesbahi, Florida International University, 20 November 2002.

[6] Martin Van Crevald, *The Transformation of War*, (New York: The Free Press, 1991), 224.

[7] Bruce D. Berkowitz and Allan E. Goodman, *Best Truth: Intelligence in the Information Age*," (London: Yale University Press, 2000), 147.

[8] Ibid., 148.

[9] Ibid., 151.

[10] Ibid.

[11] Ibid.

[12] Jacoby, *DIA Response to 9/11*, 3.

[13] Gregory F. Treverton, *Reshaping National Intelligence in an Age of Information*, (New York: Cambridge University Press, 2001), 2.

[14] Bruce Hoffman, "A Nasty Business," in *Terrorism and Counterterrorism: Understanding the New Security Environment*, ed. Russell D. Howard and Reid L. Sawyer (Guilford Connecticut, 2002), 301.

[15] Treverton, 2.

[16] Berkowitz, 148.

[17] Ibid., 160.

[18] Ken Booth, "Desperately Seeking Bin Laden: The Intelligence Dimension of the War Against Terrorism," in *Worlds in Collision: Terror and the Future of Global Order*, ed. Ken Booth and Tim Dunne (New York: Palgrave Macmillan, 2002), 72.

[19] Jacoby, *DIA Response to 9/11*, 4.

[20] Jacoby, *Sharing of Terrorism-Related Data*, 5

[21] Mr. Don Van Duyn, Chief, Counter-Intelligence Analysis Section, FBI, interview by author, 18 December 2002, Washington D.C., notes.

[22] Ibid.

[23] Deucy, 17 December 2002 Interview, NP.

[24] Andre, 18 December 2002 Interview, NP.

[25] Jacoby, *DIA Response to 9/11*, 3.

[26] Wolfowitz, *Counterterrorist Center Customer Perspective*, 3-4.

Notes

[27] Warren Rudman, "Were the Events of September 11th the Result of an Intelligence Failure," a PBS Frontline Interview, 2001, NP., On-line, Internet, 25 October 2002 Available at http://www.pbs.org/wgbh/pages/frontline/shows/terrorism/fail/why.html.

Chapter 5

Analysis, Tools, and Information

> *Accounting for and dealing with uncertainty has always been our biggest analytic challenge. But in today's environment, we need to be as adept at dealing with 'complex mysteries' as we are at uncovering 'hidden secrets.' Critical analytic thinking may be our most important national asset.*
>
> — Vice Adm Thomas R. Wilson, Statement before the Senate Armed Services Committee, 19 March 2002

The ability of talented individuals to take sometime fragmentary information and analyze potential enemy courses of action remains the bedrock of military intelligence. Key governmental decision makers and military commanders rely on intelligence professionals daily to take facts and assumptions, combine them together, and make informed inferences and assessments.[1] Painting a picture of the enemy thought process, motivation, decision patterns, and future activity is ultimately every analyst's pursuit. Regrettably, the business of terrorism provides a uniquely challenging problem in this regard. Because terrorist activity is typically sparse sometimes spanning years without appreciable data, DOD intelligence analysts must be especially adept at extracting meaning from incomplete evidence and the ever-present ambiguity.[2]

To this end, today's existing transnational terrorist threat demands a more comprehensive analytical approach in two major areas: first, we must increase our interpretive and predictive abilities within DOD; second, we must apply a broader analytical approach to studying key source data, identification features, and activity indicators for terrorism. Related to the first,

some intelligence analysts within the DOD analytical community today are doing descriptive rather than interpretive analysis.[3] That is, describing what has happened or is happening rather than discerning some deeper meaning or predictive interpretation from the activity. Due to an ever-present terrorist threat, accounting for an absence of evidence with analytic insight and creative assessments is as important today as it has ever been in the history of the DOD Intelligence Community. Analysts are counted on to recognize credible source material from chaff and make intuitive judgments sometimes based on nothing more than gut experience.[4] Unfortunately, this is easier said than done. The DOD Intelligence Community simply doesn't have enough people with the required skill base to address terrorism's distinctive analytical challenges. To some critics the problem is even simpler, asserting the basic definition of intelligence hasn't changed in over fifty years, but "almost everything else about the analyst's job has."[5]

Embracing a broader analytical approach to terrorism is recognition we are in fact dealing with a changing international environment. Globalization has provided the foundation for change by empowering individuals and small cells as never before. As former Air Force Academy Professor Maj Troy Thomas observed, "as the current war on terrorism unfolds, we are learning that war does not only involve nation-states employing lethal force to achieve political ends. The battlefield is once again an arena for a range of political entities, including violent non-state actors that may be fighting for post-heroic, apolitical reasons."[6] Clearly, violent non-state actors such as al Qaeda have changed the global canvas intelligence analysts must scour for information and meaning.

The process for producing intelligence today is still traditionally structured and somewhat isolated, and taken as a whole, lacks the necessary flexibility required to more effectively address

transnational terrorism. Because of our heritage and mission orientation for over 50 years, the intelligence culture is much more comfortable monitoring large, slowly changing threats like the former Soviet Union or North Korea. However, a more adaptable system is required to address an ever-present threat such as terrorism that can lay dormant for years and strike from unexpected quarters with very little warning.[7] Tracking individuals and networks is much different than the traditional 'intelligence preparation of the battlefield' where terrain is studied, order of battle threats are counted and identified, enemy courses of action are calculated, and so on. Analyzing an enemy with pockets of independent cells, no political or military doctrine, and no seemingly set political goals is a completely different ball game. In essence, DOD's intelligence apparatus must adapt to a new strategic context and explore new areas of information to capture and study data. The smallest detail of information cannot "be overlooked, regardless of where it might be found or how deeply imbedded in noise or obscured by faulty assumptions about its nature and relevance…the purchase or forgery of travel documents, "accidental" intrusions in secure areas, or movement of cash may have innocent explanations and benign implications. But maybe not."[8]

Successfully adapting to the analytic challenges terrorism presents is an ongoing effort within DOD. Numerous forces such as resource allocation and foreign policy decisions impact our ability to conduct counter-terrorist missions, but these influences are really outside of the category of community cultural roadblocks. Rather, within the bounds of the DOD analytic community, it is cultural inhibitors such as information access and management, and analytical skill and processes where the intelligence community needs continued change. For example, in the realm of all-source analysis, much information related to terrorism is still not subject to analytical interpretation or scrutiny within DOD today.[9] In fact, one could argue few, if any,

analysts are doing true all-source analysis within DOD, primarily due to lack of access to the raw data and material necessary to ply their trade.[10] DIA and other DOD elements are painfully aware of this situation and are aggressively trying to break this cultural paradigm. One such step taken at DIA, receiving high marks from many within the intelligence community was the standup of the Joint Intelligence Task Force—Combating Terrorism (JITF-CT).

> The single most critical goal of the JITF-CT is fielding of a stand-alone, limited access data repository accredited to host the entire range of terrorism related information, regardless of source. No such repository of information exists within the Department of Defense today. Categories of information often not subjected to all-source intelligence analysis today include some highly compartmented intelligence, law enforcement information related to ongoing investigations or prosecutions, and security incident reporting sometimes catalogued as criminal, rather than terrorism activity.[11]

Before complete, all source, interpretive terrorism analysis can take place within DOD, access to previously untapped sources of data must be achieved.

Once it is determined an analyst can have access to all relevant data available to make assessments, the problem of efficiently retrieving, manipulating, and storing the data still persists. The amount of information available regarding terrorism is overwhelming and providing an effective information management system to handle the task is no small feat. Consider the diverse organizations, various networks, separate security protocols, and differing data formats existing today within the Intelligence Community. Before access and management can begin, the real first step is agreeing on standard formats for the information, which will be used. Admiral Jacoby was adamant in stressing the need to support "the commercial world's collective embrace of extensible Markup Language—XML—it shouldn't be an elective option. Interoperability at the data level is an absolutely necessary attribute of a transformed intelligence environment because it enables horizontal integration of information from all sources—not just intelligence—and at all levels of classification."[12] Still, the need for dramatic improvements in

data management aside, we should not see technological solutions as a panacea for all-source terrorism analysis. Technology is always a double edge sword and providing access to more and more data brings with it a corresponding level of demand on the human level, both in managing the data and in analytical interpretation. Additionally, it is important to stress the limits technology can bring to the problem and the importance human analytical interpretation will always play. Data tagging and computer recognition programs are critical tools, "but the most useful indicators of terrorist threats tend to be *sui generis* ones that become apparent not in the application of a rule but in the gut of an analyst who, through experience, has acquired a feel for how a group operates."[13]

While access to all relevant terrorist data is perhaps the biggest problem confronting all source intelligence analysts today, we must also be concerned about the potential for overloading analysts with too much information. Given the two extremes, the DOD intelligence professional will of course take all the information we can get. Still, intelligence analysis is a difficult profession fraught, like just about any other, with potential pitfalls. The scope of this effort is beyond a detailed study of the psychology of intelligence analysis; however, two areas of potential concern warrant mentioning, especially in regard to terrorism: first, the desire for tactical warning of terrorist activity and near-term answers may lead analysts to provide incremental or incomplete assessments and; second, an effort focused on tactical solutions may preclude a further strategic, or comprehensive study of the available information.

As previously noted, terrorism-related analysis requires looking at numerous sources of data not normally associated with the traditional role of intelligence analysis. The requirement to review vast amounts of data is compounded by the fact that the increasing threat of transnational terrorism brings with it a growing responsibility to provide timely indications and warning of

potential attacks. Globalization and technology have built a world where we want access to information and answers now, not later. The American people deserve as much for strategic notification provides little reassurance with respect to terrorism, the nature of the threat demands timely and specific warning.[14] The daily concern for intelligence professionals is making sure the timely and specific warning is accurate.

It is a given support to military operations and analysis of terrorist indications clearly requires a timely, tactical perspective. Alternatively, we must also ensure an element of strategic depth is applied, using source data and information analyzed over longer periods of time, to study terrorist historical patterns and cultural influences. Failure to support tactical assertions with strategic depth built on experience can result in what former CIA analyst Richards J. Heuer, Jr. calls incremental analysis. According to Heuer, the intelligence professional's preconceptions about an event or issue have a greater impact on an analytical product than analysts from other fields working with less ambiguous or missing information.[15] When bits of information are examined piecemeal, without the benefit of time or a comprehensive look, the final product or interpretation may be incomplete or misleading. An example is offered from analysis of the Arab-Israeli War of 1973 where it was noted the problem of incremental analysis was "analysts, according to their own accounts, were often preceding on the basis of the day's take, hastily comparing it with material received the previous day. They then produced in 'assembly line fashion' items which may have reflected perceptive intuition but which [did not] accrue from a systematic consideration of an accumulated body of integrated evidence."[16]

Incremental analysis is very closely related to another possible analytical pitfall, something psychologists call premature closure. Premature closure generally refers to arriving at a quick assessment before sufficient hard information is available to make possible a well-informed

appraisal.[17] Granted, the heart of an intelligence analyst job is to compensate for the lack of existing and obvious evidence.[18] However, today's dynamic threat environment characterized by fragmentary data and charged with political pressure for answers has potential for incomplete assessments based on limited information. It is not inconceivable to envision a scenario where analysts may feel pressure to provide some type of answer, even if any appreciable evidence or information is lacking. In assessing an event or threat, it is critical for analysts to outline for decision makers and commanders what they don't know, as well as what they do know. It is a simple reality that specific data or indicators will sometimes be lacking, especially in regard to the dynamic and veiled puzzle that is global terrorism. As Bruce D. Berkowitz and Allan E. Goodman observe, "it is the job of intelligence specialists to define facts, gaps in facts, and the logical conclusion of facts. It is the job of public officials to make judgments about risk and articulate their judgments to the public."[19] As a national security community or even more broadly, as a nation, we need to invest more energy in educating the United States public at large about the risks of terrorism and our ability to mitigate those risks.

Like just about every other discipline in DOD, the resource-strapped intelligence apparatus of the 1990s and early twenty-first century had to find new and inventive ways of doing business. One of the most successful processes used was called federation or collaboration, and involved dividing up the workload between various organizations within the DOD Intelligence Community. For example, if 100 pieces of information required study, 40 might be looked at by DIA, Unified Commands such as Strategic Command or Pacific Command would do 30, and 30 more might be done by a Service, such as the Air Force. For senior leaders and military commanders, the key attraction federation offers to these labor-intensive processes is to

maximize resources while reducing duplication of effort. Each organization would be given a piece of the pie to address; competitive analysis or overlap is expected to be minimal.

The general opinion of many key intelligence officials, however, is that federation doesn't work for terrorism analysis. "While some issues are prime candidates for cross-community economizing—i.e. distributed or federated analysis, product deconfliction, strict division of labor—terrorism is not one of them…terrorism is an issue where competitive analysis is essential; planned duplication and redundancy are virtues."[20] Part of this contention no doubt rests on the fact DOD does not have enough experienced and trained terrorism analysts. More likely though, is the complexity and challenge terrorism provides as an area of analysis, one where redundancy is beneficial or even necessary. Data considered irrelevant by one analyst may be a treasure trove of information and provide critical clues or reveal significant relationships for another.[21] Of course redundancy or competitive analysis requires a common framework from which to proceed. Improved information access, a diverse and well-trained work force, utilization of new data sources, and leadership willing to accept differing points of view will ultimately be the acid test for improving the DOD Intelligence Community's ability to prosecute the war on terrorism.

Notes

[1] Andre, 18 December 2002 Interview, NP.
[2] Jacoby, *Sharing of Terrorism-Related Data*, 3.
[3] Andre, 18 December 2002 Interview, NP.
[4] Mr. Robert Boyd, Director of Intelligence Analysis, Headquarters Air Force, interview by author, 18 December 2002, Washington D.C., notes.
[5] Berkowitz, 99.
[6] Maj Troy Thomas et al, "Lords of the Silkroutes," (an unpublished monograph, n.d.), NP.
[7] Berkowitz, 63.
[8] Jacoby, *DIA Response to 9/11*, 3.
[9] Andre, 18 December 2002 Interview, NP.
[10] Ibid.
[11] Jacoby, *Sharing of Terrorism-Related Data*, 2.

Notes

[12] Ibid., 8.
[13] Paul Pillar, *Terrorism and U.S. Foreign Policy*, (Washington D.C.: Brookings Institute Press, 2001), 113.
[14] Jacoby, *DIA Response to 9/11*, 2.
[15] Richard J. Heuer Jr., *Psychology of Intelligence Analysis*, (Washington D.C.: Center for the Study of Intelligence, Central Intelligence Agency, 1999), 14-15.
[16] Ibid., 15.
[17] Ibid., 16.
[18] Andre, 18 December 2002 Interview, NP.
[19] Berkowitz, 164.
[20] Jacoby, *DIA Response to 9/11*, 3.
[21] Jacoby, *Sharing of Terrorism-Related Data*, 7.

Chapter 6

Prescriptions for the Future

> *What I envision is a different way of doing business in the intelligence and Law Enforcement communities. Make no mistake; it would involve unfamiliar processes, partnerships, and prerogatives.*
>
> —Rear Adm Lowell E. Jacoby, Written Statement for the "Joint 9/11 Inquiry," 1 October 2002.

Improving DOD's capability to combat terrorism requires a continuing intellectual shift in the minds of many intelligence professionals. Grasping the impact of globalization; recognizing the characteristics of, and changes in, an unpredictable and shadowy terrorist enemy; and struggling with the subtle nuances of changing relationships between traditionally separate segments of the Intelligence Community will all take time and energy. Thus, four major areas of focus will ultimately determine our ability to make the necessary cultural shift within DOD: the training and recruitment of analysts; the engagement of sources outside of the traditional analytic realm such as the Internet and academic scholars; the breaking down of unnecessary compartmentalization between sister intelligence organizations; and for lack of better terminology, 'expectation management' of governmental leaders and the American public.

As a whole, DOD requires a more aggressive and broad-based recruitment and training programs for the intelligence career field. Granted, some organizations have made great strides in an effort to bring in the best and brightest candidates. Particularly notable are DIA's efforts as part of their 'revitalizing the workforce,' one of the director's four focus areas for the

organization. DIA visits about 95 academic institutions per year and provides some scholarship assistance for students.[1] As part of this program, DIA is also working to bring in more 'fringe elements' to address language and cultural gaps in its workforce.[2] The uniformed services acquire intelligence officers through a less rigorous selection process; either via Officer Training Schools, the Reserved Officer Training Corp (ROTC) program, the various military academies, or from other career paths. The Air Force for example has many intelligence officers who were slated to be pilots but did not make it through flight training. Most turn out to be excellent intelligence officers, however, the point is the recruitment, acquisition, and training of intelligence personnel, focusing on analytic skill or cultural diversity, doesn't seem to be an overriding priority from day one. In ROTC for example, students can apply for an intelligence job only after their junior year of school. Even when looking at DIA, the process for DOD seems somewhat limited. Usually a pool of potential talent is developed, mostly from college graduates or individuals about to graduate college at one institution or another who are then recruited for a career as an intelligence specialist. The question remains, is this process the best way to deliver the analytical skills necessary to confront global terrorism over the long-term?

The rigorous diagnostic requirements required of todays, and no doubt future intelligence analysts, require earlier and more focused recruitment and training programs. Largely because of the September 11 tragedies, we find ourselves in an era filled with patriotism, an era fertile for recruiting.[3] More than ever, Americans want to do something to aid in the battle against terrorism. Still, as decades of experience have shown, public opinion can wane, especially if the perception prevails that the threat has lessened. While the timing is right, we need to establish more structured processes for acquiring culturally diverse and skilled intelligence analysts just as we have for pilots or nuclear submarine captains. The mission requirements today are just that

important. DOD should identify and recruit more candidates out of high school for specific intelligence career tracks specially designed at the military academies or selected universities. Perhaps part of their summer internships could be spent at DIA, abroad at various embassies, or with a service unique intelligence agency getting oriented to the requirements of an intelligence specialist. Along with flight training opportunities or parachute jump training, such as those offered at the Air Force Academy, certain students could receive specialized instruction and training from DIA's Defense Intelligence College. It is understood granting certain security clearances would be impossible, however, mechanisms could be worked out providing certain levels of access.

Similarly, funding and scholarships at universities should be greatly expanded for the sole purpose of creating intelligence analysts. Understandably, some institutions may shy away from overt relationships with intelligence organizations, but some may not. The State Department has numerous programs for Foreign Service Officers and DOD has well-established ROTC programs within many universities. DOD intelligence agencies should become more involved with these programs or conceivably begin one of our own. Selecting potential talent going into college rather than just choosing from the pool of candidates coming out of college has major potential benefits. The basic prerequisites for a good intelligence analyst; curiosity, passion, and creativity can easily be identified early and then nurtured.[4] Augmenting the educational experience with study abroad or summer assignments to Embassies or Consulates can only enrich the cultural understanding of perspective candidates. "The only certain way to increase the breadth and diversity of assumptions is to increase the breadth and diversity (in terms of education and experiential background, cultural values, intellectual biases, etc.) of the analysts involved in the assessment process."[5]

The second major area requiring cultural vectoring is an increased utilization of non-traditional intelligence sources such as the Internet, American and foreign scholars, and other open-source materials. Somewhat related is the need for increased and more in-depth exchanges with foreign government security and intelligence agencies, but again as a result of September 11, this is an area where much progress has been made.[6] The basic reasoning for the above assertion is the differing analytic challenge terrorism brings as opposed to traditional state-centered intelligence exploitation. All relevant and truly beneficial information regarding terrorist intentions won't just be found behind a state-sponsored iron curtain of silence. Transnational terrorist cells may leave relatively overt clues by having specifically relevant cultural ties, by relying heavily on unclassified networked communication, or even by using planning data or information available to the general public. DOD must become proficient, much akin to traditional skills found in the Law Enforcement Community, in knowing how to look and where to find pertinent, unclassified, intelligence information. This is not to say DOD needs to become a research agency daily plowing through mounds of data available through open source channels. We just need to know largely untapped resources such as the Internet have potential merit in the battle against terrorism, and understanding where data can be found, who can best help in this regard, and how to use the data, are all critical.

Forging relationships and establishing contacts to help this process may not always be easy however. Some experts in business or academia may be eager to help intelligence organizations but both parties may be disinclined to have any direct association. Therefore, it may be necessary to work through intermediaries such as other government or some private organizations.[7] Nay sayers to developing the aforementioned associations will always persist on both sides of the argument. Nonetheless, the potential long-term benefits of relationships with

foreign or American scholars should not be dismissed out of hand. As Richard Betts asserts, "No one can match the analysts from the CIA, the Defense Intelligence Agency (DIA), or the NSA in estimating bin Laden's next moves, but it is not clear that they have a comparative advantage over Middle East experts in think tanks or universities when it comes to estimating worldwide trends in radical Islamist movements over the next decade. Such long-term research is an area in which better use of outside consultants and improved exploitation of academia could help most."[8]

As important as expanding our recruitment base and use of non-traditional sources of intelligence data are, breaking down unnecessary compartmentalization and improving analytic perspective through information sharing is even more so. Two fundamental changes within the Intelligence Community are necessary to achieve this goal; first, an assessment of and decision on what can be shared by appropriately identified parties and; second, implementing the technological solutions enabling individual analysts to access, manipulate, share, and store data quickly and easily. As expressed by Admiral Jacoby, "If we expect analysts to perform at the level and speed expected in a counterterrorism mission environment characterized by pop-up threats, fleeting targets, and heavily veiled communication, they require immediate, on-demand access to data from all [sic] sources and the ability to mine, manipulate, integrate, and display all relevant information."[9]

For obvious and extremely valid reasons, the intelligence world operates under the security banner of 'need to know.' Information must be controlled and shared with ever-present concern of compromise guiding each step of the process. Still, within these grounded prerequisites, the greater Intelligence Community needs to find ways to reduce unnecessary compartmentalization and share information within its membership. Transnational terrorism brings a multi-faceted,

diffuse, and continuously evolving threat manifested by interconnected groups and individuals with global reach. Analytic assessments and interpretative understanding is critically dependent on successful cooperation between CIA, DIA, FBI, and all other agencies involved in terrorism-related intelligence work. Only by developing comprehensive data bases and setting operational processes for using this information will the Intelligence Community maximize its potential to confront and manage the terrorist enemy. For mission execution in DOD the equation is simple, the analytic component can play a more significant role in combating terrorism only if given access to a greater array of information and supported with more capable tools to manipulate this information.[10] Because terrorism analysis demands a centralized, competitive approach, has a large diversity of intelligence community actors involved, is dependent on breaking into the 'information ownership' paradigm of these other intelligence organizations, and has a global playing field, DIA must continue to lead the required cultural shift for DOD terrorism analysis.

The last major cultural area impacting DOD's ability to combat transnational terrorism is expectation management. This terminology simply refers to understanding the limitations of intelligence agencies and analysts. Despite the desires of some statesman and commanders, and our own efforts to improve analysis, access to information, and data management, intelligence professionals can't provide answers or indicators all of the time. This is especially true of terrorism and tactical warning where sometimes there are no indicators. As former Senator Rudman articulated during an interview with the Brookings Institute, "Understand the duties of intelligence agencies. We have to know about people's capabilities. We have to know about their capacity to injure us. We would like to know their intentions. But I will repeat to you: We do find out intentions some of the time, but not all of the time. And in this business -- it's a zero-sum

business -- if you don't find it all the time, then what happened in New York is what will happen again, chilling as that may be."[11]

So what can be done to assist the DOD analytical community in this endeavor? There are several issues that may deserve attention, but two broad areas are paramount. The first is education of the public, a matter that has made tremendous strides since September 11th. Prior to this time, the intelligence and law enforcement communities were waging a battle without an alert and committed American public, perhaps the most important weapon needed in this effort.[12] The Bush administration's efforts over the last 18 months have done much to alleviate this situation. Nonetheless, it is vital we remain committed to educating our citizenry about the complexities of terrorism, in the form of warning as well as in the challenge it presents for our government, military forces, and Intelligence Community. This is especially important today because, as witnessed by Secretary Powell's recent appearance before the United Nations Security Council, intelligence information is being used more and more in public debates concerning global policy decisions.[13]

A somewhat related second area is as old as war itself, meeting the expectations of government leaders and commanders. Most every senior decision maker in the United States government or DOD is aware of the unique challenges terrorism presents for intelligence analysts. Still, the desire for information, quick assessments and timely warnings has never been greater. As Deputy Secretary of Defense Wolfowitz expressed before Congress:

> We must also accelerate the speed with which information is passed to policymakers and operators. We cannot wait for critical intelligence to be processed, coordinated, edited and approved—we must accept the risks inherent in posting critical information before it is processed…we need a more transparent process, one that gets alternative analyses up on the table quickly for policy makers to grapple with. We should not make the mistake of assuming that good intelligence analysis must arrive at definitive or agreed conclusions…and we need

> to avoid making the mistake of thinking that intelligence estimates reached by consensus should routinely trump those of a lone dissenting voice. They don't.[14]

Unmistakably, alternative analysis and timely transmission of information to decision makers is paramount to combating terrorism. However, delivering "unprocessed" critical information and numerous "unapproved" alternative perspectives is not without risk. It puts even more pressure on key leaders for decisions, especially during events or contingencies where the timeline for a judgment is short. Knowing terrorist information will many times be fragmentary, decision-makers will often find themselves forced to make, and stand behind, decisions without all available information. For that reason, the next scenario couched as an intelligence failure, and there will be one, must take the form of we or us versus them or it. For the process of intelligence revolves so much around decision making and real Intelligence Community is inextricably woven and complex, made up of not just the traditionally identified organizations (CIA, DOD, FBI, etc), but by all facets of government, public influences, and influential leaders whose decisions very much impact it.

Notes

[1] Andre, notes.
[2] Ibid.
[3] Boyd, notes.
[4] Andre, notes.
[5] Jacoby, *Sharing of Terrorism-Related Data*, 4.
[6] Deucy, notes.
[7] Berkowitz, 57.
[8] Betts, *Fixing Intelligence*, 477.
[9] Jacoby, *Sharing of Terrorism-Related Data*, 7.
[10] Jacoby, *DIA Response to 9/11*, 3.
[11] Rudman, NP.
[12] Hill, *Response to Past Terrorist Attacks*, 2.
[13] Berkowitz, 100.
[14] Wolfowitz, 4-5.

Chapter 7

Conclusion

> *As of today, we're changing the laws governing information sharing. And as importantly, we're changing the culture of our various agencies that fight terrorism. Countering and investigating terrorist activity is the number one priority for both law enforcement and intelligence agencies.*
>
> —President George W. Bush, Remarks at the Signing of the Patriot Act, Anti-Terrorism Legislation, 26 October, 2001

Existing cultural practices and compartmentalized operational processes within the DOD Intelligence Community, long successful in dealing with nation-state threats such as the former Soviet Union, were exposed on September 11, 2001 as insufficient in confronting the technologically empowered terrorist threat. Still apparent today, DOD's analytic intelligence community requires a continuing cultural shift to more effectively prosecute the war on terrorism and strengthen America's national security. Great progress has been made since the tragic events of 18 months ago, however, much still needs to be done to meet President Bush's goal of changing governmental agency cultures to fight terrorism. DOD alone cannot accomplish this burden of cultural change within its analytic community. Shifting DOD's cultural makeup and practices will rely as much on the greater Intelligence Community and other government bureaucracies, as from its own internal adaptation.

Changing the mindset and operational practices of any large bureaucracy is a great challenge and obviously will take time. Therefore, as important as recognition for cultural change is, true progress cannot be made without deep steadfastness of purpose from the Executive and

Legislative branches of government, the greater Intelligence Community, and the DOD itself over an extended time period. "The war on terrorism is a long-term proposition that demands extraordinary continuity of purpose, focus and resource commitment."[1] Remaining vigilant and maintaining a steady state regarding recruiting, training, information sharing, reduced compartmentalization, and the like, will in due course prove the key to success.

Along with many deeply felt emotions, the tragedy of September 11 brought about the revelation the world has indeed changed, as has the twenty-first century terrorist enemy. Globalization and technology have given small groups and individuals enormously increased capabilities, even the power to influence great nation-states. Correspondingly, the requirements and timelines for intelligence the military needs to combat terrorism have also changed. To respond effectively to these changes, the DOD Intelligence Community must adapt its culture to meet this mounting challenge. The risk of not adapting is being left behind as the war against terrorism progresses, or worse yet, being labeled as irrelevant by the rest of DOD in supporting critical military requirements and operations.

Notes

[1]Jacoby, *DIA Response to 9/11*, 1-2.

Glossary

AU	Air University
CIA	Central Intelligence Agency
DCI	Director, Central Intelligence Agency
DIA	Defense Intelligence Agency
DOD	Department of Defense
FBI	Federal Bureau of Investigations
FEMA	Federal Emergency Management Agency
GPO	Government Printing Office
HUMINT	Human Intelligence
IC	Intelligence Community
I&W	Indications and Warning
JIC	Joint Intelligence Center
JITF-CT	Joint Interagency Task Force-Counterterrorism
NAIC	National Air Intelligence Center
NGIC	National Ground Intelligence Center
NSA	National Security Agency
NSS	National Security Strategy
PDD	Presidential Decision Directive
ROTC	Reserve Officer Training Corp
U.S.	United States
USCENTCOM	United States Central Command
WTC	World Trade Center

XML	Extensible Markup Language
9/11	September 11, 2001

Selected Bibliography

Berkowitz, Bruce D. and Goodman, Allan E, *Best Truth: Intelligence in the Information Age*, London: Yale University Press, 2000.

Best Jr., Richard A., "Intelligence to Counter Terrorism" Congressional Research Service, The Library of Congress, CRS Web at http://www.fas.org/irp/RL312292.pdf, February 21, 2002.

Betts, Richard K., "The Soft Underbelly of American Primacy: Tactical Advantages of Terror," in Russell D. Howard and Reid L. Sawyer Eds., *Terrorism and Counterterrorism: Understanding the New Security Environment*, Guilford Connecticut, McGraw-Hill/Dushkin, 2002, pp. 338-353.

Betts, Richard K., "Fixing Intelligence" in Russell D. Howard and Reid L. Sawyer Eds., *Terrorism and Counterterrorism: Understanding the New Security Environment*, Guilford Connecticut, McGraw-Hill/Dushkin, 2002, pp. 473-482.

Booth, Ken, "Desperately Seeking Bin Laden: The Intelligence Dimension of the War Against Terrorism" in Ken Booth and Tim Dunne Eds., *Worlds in Collision: Terror and the Future of Global Order*, New York: Palgrave Macmillan, 2002.

Bremer, Paul L. III, Ambassador, Chairman, National Commission on Terrorism, Testimony before the United States Senate, Select Committee on Intelligence at http://fas.org/irp/congress/2000_hr/000608_bremer_terrorism.html, June 8, 2000.

Bush, George W. "President Signs Anti-Terrorism Bill," Remarks at Signing of the Patriot Act, Anti-Terrorism Legislation, The East Room, Washington, DC at http://www.whitehouse.gov/news/releases/2001/20011026-5.html, October 26, 2001.

Carter, Ashton B., "The Architecture of Government in the Face of Terrorism" in Russell D. Howard and Reid L. Sawyer Eds., *Terrorism and Counterterrorism: Understanding the New Security Environment*, Guilford Connecticut, McGraw-Hill/Dushkin, 2002, pp. 428-441.

Deutch, John and Smith, Jeffrey H., "Smarter intelligence, " in Foreign Policy Magazine at http://www.foreignpolicy.com/issue_janfeb_2002/deutch.html, 2002.

Donohue, Laura K., "Fear Itself: Counterterrorism. Individual Rights, and U.S. Foreign Relations Post 9-11," in Russell D. Howard and Reid L. Sawyer Eds., *Terrorism and Counterterrorism: Understanding the New Security Environment*, Guilford Connecticut, McGraw-Hill/Dushkin, 2002, pp. 275-300.

Goss, Porter, Chairman, House Permanent Select Committee on Intelligence, "Need for Human Intelligence," a Frontline Interview available at http://www.pbs.org/wgbh/pages/frontline/shows/terrorism/fail/why.html, 2001.

Heuer Jr., Richard J., *Psychology of Intelligence Analysis*, Washington D.C.: Center for the Study of Intelligence, Central Intelligence Agency, 1999.

Hill, Eleanor, Staff Director, Joint Inquiry Staff, "Hearing on the Intelligence Community's Response to Past Terrorist Attacks Against the United States from February 1993-September 2001," Statement before the Joint Hearing of the United States Senate Select Committee on Intelligence and the United States House Permanent Select Committee on Intelligence at http://fas.org/irp/congress/2002_hr/100802hill.html, October 8, 2002.

Hill, Eleanor, Staff Director, Joint Inquiry Staff, "Hearing on the Intelligence Community's Response to Past Terrorist Attacks Against the United States from February 1993-September 2001," Statement before the Joint Hearing of the United States Senate Select Committee on Intelligence and the United States House Permanent Select Committee on Intelligence at http://fas.org/irp/congress/2002_hr/101702hill.html, October 17, 2002.

Hoffman, Bruce, *Inside Terrorism*, New York: Columbia University Press, 1998.

Hoffman, Bruce, "A Nasty Business," in Russell D. Howard and Reid L. Sawyer Eds. *Terrorism and Counterterrorism: Understanding the New Security Environment,* Guilford Connecticut, McGraw-Hill/Dushkin, 2002, pp. 301-306.

Hughes, Patrick M., Lt Gen (Retired), Prepared Testimony for the United States Senate Committee on Governmental Affairs at http://fas.org/irp/congress/2002_hr/062602hughes.html, 26 June 2002.

Jacoby, Rear Adm Lowell E., Acting Director, Defense Intelligence Agency, "The Joint 9/11 Inquiry," *Information Sharing of Terrorism-related Data*, Written Statement for the Record before the Joint Hearing of the United States Senate Select Committee on Intelligence and the United States House Permanent Select Committee on Intelligence at http://fas.org/irp/congress/2002_hr/100102jacoby.html, October 1, 2002.

Jacoby, Rear Adm Lowell E., Acting Director, Defense Intelligence Agency, "The Joint 9/11 Inquiry," *DIA Response to Joint 9/11 Letter of Invitation*, Written Statement for the Record before the Joint Hearing of the United States Senate Select Committee on Intelligence and the United States House Permanent Select Committee on Intelligence at http://fas.org/irp/congress/2002_hr/101702jacoby.html, October 17, 2002.

Pillar, Paul R., *Terrorism and U.S. Foreign Policy*, Washington D.C.: Brookings Institution Press, 2001.

Rudman, Warren, Former Senator, "Were the Events of September 11th the Result of an Intelligence Failure," a Frontline Interview available at http://www.pbs.org/wgbh/pages/frontline/shows/terrorism/fail/why.html, 2001.

Schultz, Richard H. and Vogt, Andreas, "The Real Intelligence Failure on 9/11 and the Case for a Doctrine of Striking First," in Russell D. Howard and Reid L. Sawyer Eds. Terrorism and Counterterrorism: Understanding the New Security Environment, Guilford Connecticut, McGraw-Hill/Dushkin, 2002, pp.367-390.

Smith, Jeffrey, Former General Counsel of the CIA, "Constraints and Obstacles Facing U.S. Intelligence," Excerpts from Frontline Interviews available at http://www.pbs.org/wgbh/pages/frontline/shows/terrorism/fail/constraints.html, 2001.

Tenet, George, Director of Central Intelligence, "Joint Inquiry Committee," Written Statement for the Record before the Joint Hearing of the United States Senate Select Committee on Intelligence and the United States House Permanent Select Committee on Intelligence at http://fas.org/irp/congress/2002_hr/101702tenet.html, October 17, 2002.

The White House, *A National Security Strategy for a Global Age*, December 2000.

The White House, *The National Security Strategy of the United States of America*, September 2002.

Thomas, Troy, et al, "Lords of the Silkroutes," an unpublished Monograph, 2002.

Treverton, Gregory F, RAND, Reshaping National Intelligence in an Age of Information, New York: Cambridge University Press, 2001.

Senate, The Committee on Foreign Relations, Strategies for Homeland Defense: A Compilation by the Committee on Foreign Relations, 107th Congress, 1st sess., Washington, GPO, 26 September 2001.

Van Crevald, Martin, *The Transformation of War*, New York: The Free Press, 1991.

Wilcox, Philip C. Jr., Ambassador, Coordinator for Counterterrorism, "Combating International Terrorism," Statement for the record before the United States House of Representatives, Permanent Select Committee on Intelligence at http://fas.org/irp/congress/1996_hr/h960305w.html, March 5, 1996.

Wilson, Vice Adm Thomas R., Director, Defense Intelligence Agency, "Global Threats and Challenges Through 2015," Statement for the Record before the Senate Armed Services Committee at http://fas.org/irp/congress/2001_hr/s010308w.html, 8 March 2001.

Wilson, Vice Adm Thomas R., Director, Defense Intelligence Agency, "Global Threats and Challenges Through 2015," Statement for the Record before the Senate Armed Services Committee at http://fas.org/irp/congress/2002_hr/031902wilson.html, 19 March 2002.

Wolfowitz, Paul, Deputy Secretary of Defense, "Joint Inquiry Hearing on Counterterrorist Center Customer perspective," Prepared Testimony for the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence at http://fas.org/irp/congress/2002_hr/091902wolfowitz.html, September 19, 2002.

Woolsey, James R., former Director of Central Intelligence, Statement before United States House of Representatives Committee on National Security, available at http://fas.org/irp/congress/1998_hr/h9800212w.html, February 12, 1998.

An interview with Mr. Louis Andre, Chief Operating Officer, Defense Intelligence Agency, conducted 18 December 2002 by Lt Col Jack L. Jones (notes were used for this information).

An interview with Mr. Robert Boyd, Director of Intelligence Analysis, Headquarters Air Force, conducted 18 December 2002 by Lt Col Jack L. Jones (notes were used for this information).

An interview with Mr. Charles P. Duecy, Director, Joint Intelligence Task Force—Combating Terrorism, DIA, conducted 17 December 2000 by Lt Col Jack L. Jones (notes were used for this information).

An interview with Mr. Don Van Duyn, Chief, Counter-Intelligence Analysis Section, FBI, conducted 18 December 2002 by Lt Col Jack L. Jones (notes were used for this information).

An interview with Admiral Murrett, Vice Director for Intelligence, J2, Joint Chiefs of Staff, conducted 17 December 2002 by Lt Col Jack L. Jones (notes were used for this information).

An interview with Colonel Jon Wohlman, Deputy Director, Intelligence Assessments, Doctrine, Requirements and Capabilities, J2, Joint Chiefs of Staff, conducted 18 December 2002 by Lt Col Jack L. Jones (notes were used for this information).

From notes taken by Lt Col Jack L. Jones during lecture by Professor Mohiaddin Mesbahi, class on National Security, Florida International University, 20 November 2002.